securonix

SOLUTION BRIEF

Amazon Web Services (AWS) Security Monitoring

As with most public clouds, Amazon Web Services provides services to detect traditional cybersecurity attacks. However, AWS is vulnerable to insider threats such as credential compromise and data exfiltration. Additionally, AWS security monitoring services are fragmented and complex, so it's hard to get a holistic view of AWS cloud monitoring detection and response.

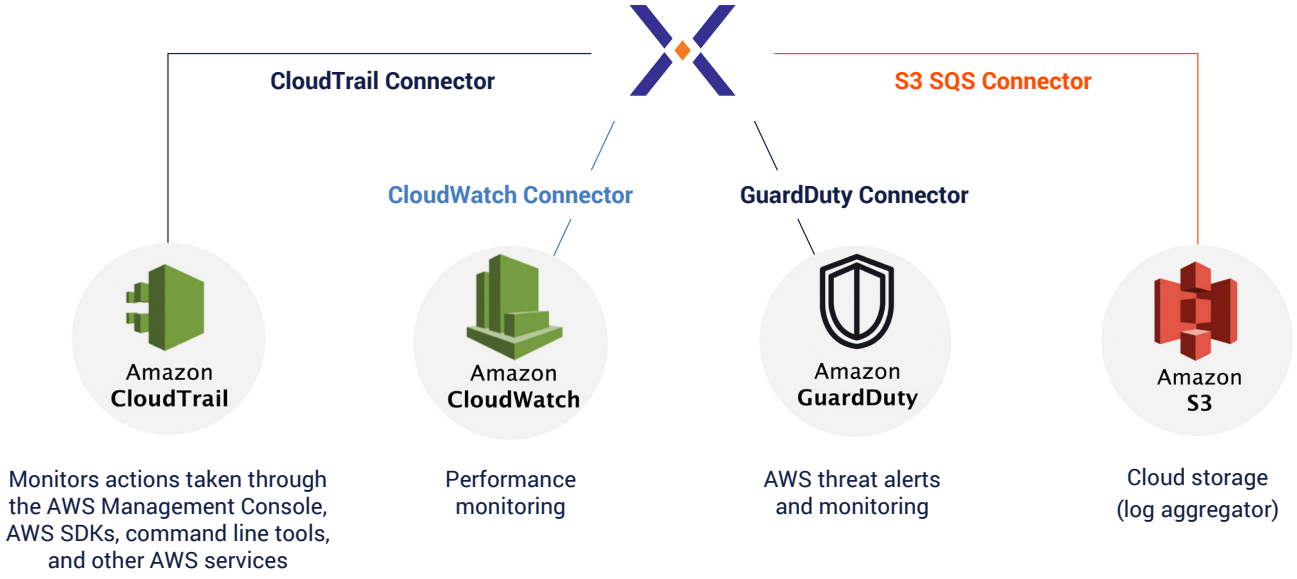
To help organizations gain visibility into their AWS infrastructure, and detect advanced cybersecurity attacks, Securonix offers customers a tightly integrated security monitoring solution. Securonix uses bi-directional integration with AWS components to provide end-to-end security monitoring, advanced threat detection, data retention, and automated incident response capabilities.

Securonix has a direct API integration with AWS, allowing Securonix to collect and analyze logs across various AWS products. Securonix then combines this information with additional context in order to quickly detect AWS-linked security events including data compromise, unauthorized access attempts, suspicious traffic, and many others.

This gives you complete visibility into your AWS environment in a single glance.

Securonix integrates with:

- **Amazon CloudTrail:** Monitors API calls to the AWS platform from around 154 different services.
- **Amazon CloudWatch:** Provides performance monitoring, such as CPU and disk usage, as well as other log types.
- **Amazon Simple Storage Service (S3):** Manages log storage from multiple sources, such as CloudFront, web application firewall (WAF), Elastic Load Balancer (ELB), and CrowdStrike.
- **Amazon GuardDuty:** Organizes monitoring and alert generation.



Key Cases

- Unauthorized access such as a login from a rare IP or geolocation, a spike in failed logins, a land speed anomaly, or a malicious IP.
- Amazon EC2 configuration anomalies such as a spike in instance creation or deletion, suspicious admin activities, or a rare instance.
- Suspicious AWS IAM activity such as suspicious user creation, admin privilege changes, password policy changes, or rare privileged activity.
- Anomalous API connections including from a rare IP or geolocation, or a malicious IP address.
- Suspicious Amazon VPC traffic including port scans or connections on anomalous ports.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization.

For more information visit www.securonix.com.

AWS Validated Security Competency

Securonix is an Amazon Web Services (AWS) Security Competency Partner. This designation recognizes that Securonix has demonstrated technical proficiency and proven customer success in delivering next-generation SIEM as a service on the AWS platform.

Achieving AWS Security Competency differentiates Securonix as an AWS Partner Network (APN) member that offers specialized software designed to help organizations adopt, develop, and deploy complex security projects on AWS. To receive the designation, APN partners must possess deep AWS expertise and deliver solutions seamlessly on AWS.

aws marketplace

Visit Securonix in AWS Marketplace

aws partner network

Advanced Technology Partner

Security Competency

securonix